

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Reguvis Fachmedien GmbH
Amsterdamer Str. 192
50735 Köln

www.reguvis.de

Beratung und Bestellung:
E-Mail: wirtschaft@reguvis.de

ISBN (Print): 978-3-8462-0906-6

© 2023 Reguvis Fachmedien GmbH

© 2023 Bundesamt für Sicherheit in der Informationstechnik, Bonn

Alle Rechte vorbehalten. Das Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der Grenzen des Urheberrechtsgesetzes bedarf der vorherigen Zustimmung des Verlags. Dies gilt auch für die fotomechanische Vervielfältigung (Fotokopie/Mikrokopie) und die Einspeicherung und Verarbeitung in elektronischen Systemen. Hinsichtlich der in diesem Werk ggf. enthaltenen Texte von Normen weisen wir darauf hin, dass rechtsverbindlich allein die amtlich verkündeten Texte sind.

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik, Bonn

Gesamtverantwortung und Chefredaktion: Holger Schildt

Redaktion: Stefanie Förster, Brigitte Hoffmann, Johannes Oppelt und Jessika Welticke

Erstellung und Aktualisierung von IT-Grundschutz-Bausteinen: Petra Bottenberg, Alex Didier Essoh, Stefanie Förster, Daniel Gilles, Florian Göhler, Florian Hillebrand, Brigitte Hoffmann, Cäcilia Jung, Birger Klein, Alexander Nöhles, Johannes Oppelt und Christoph Wiemers

Herstellung: Günter Fabritius

Satz: Cicero Computer GmbH, Bonn

Druck und buchbinderische Verarbeitung: Plump Druck & Medien GmbH, Rheinbreitbach

Printed in Germany

Vorwort

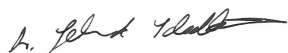
Der IT-Grundschutz des BSI beleuchtet inzwischen seit fast 30 Jahren Themen und Entwicklungen in der Informationssicherheit und leitet daraus praktikable Sicherheitsempfehlungen ab. Institutionen, die in Zeiten der Digitalisierung ihre Prozesse und Projekte nach dem Stand der Technik absichern wollen, finden hier ein umfangreiches Instrumentarium. Eine erfolgreiche und nachhaltige Digitalisierung kann nur gelingen, wenn Sicherheitsanforderungen – wie sie im IT-Grundschutz des BSI beschrieben sind – frühzeitig mitgedacht und erfüllt werden. Damit ist diese bewährte BSI-Methode sowohl Voraussetzung als auch leichter Einstieg und Nachschlagewerk, um den Herausforderungen der Digitalisierung zu begegnen.

Da ist es wenig verwunderlich, dass es in immer mehr Anwendungsfeldern IT-Grundschutz-Profile gibt, wie zum Beispiel für Weltrauminfrastrukturen. Es beschreibt Mindestanforderungen an die Cyber-Sicherheit für Satelliteninfrastrukturen. Eine Arbeitsgruppe bestehend aus Expertinnen und Experten von BSI, OHB Digital Connect, Airbus Defence and Space und von der Deutschen Raumfahrtagentur im Deutschen Zentrum für Luft- und Raumfahrt (DLR) erstellte das Profil. Weitere Beispiele sind IT-Grundschutz-Profile zur Absicherung von 5G-Campusnetzen oder für Verkehrssteuerungs- und Leitsysteme der Bundesautobahn, die alle auf den Bausteinen des IT-Grundschutz-Kompodiums basieren. Anwenderinnen und Anwender aus Wirtschaft und Verwaltung erhalten darin praxisnahe Empfehlungen und Informationen.

Mit der vorliegenden Ausgabe des IT-Grundschutz-Kompodiums steht Zuständigen in Behörden und Unternehmen erneut ein fundiertes Werkzeug mit einer breiten, aktuellen und geprüften Expertise zu allen Facetten der Informationssicherheit zur Verfügung. So können Sie die relevanten Aufgaben angehen: Erste Schritte zur Absicherung von Gebäuden, IT-Systemen und Datennetzen, der Aufbau eines Managementsystems zur Informationssicherheit oder der Schutz von besonders sensiblen Informationen. Mit den bewährten und praxistauglichen Empfehlungen des IT-Grundschutzes im IT-Grundschutz-Kompodium sind Sie gut gerüstet.

Das IT-Grundschutz-Kompodium wurde überarbeitet und um wichtige, neue Themen, wie Virtualisierung, ergänzt, die nun anhand von praxisbewährten Anforderungen in eigenständigen Bausteinen behandelt werden. Vorhandene Bausteine, wie zum Outsourcing, wurden grundlegend überarbeitet. Hinzu kommen zahlreiche weitere Ergänzungen und Aktualisierungen, die auf der Grundlage des Anwenderbedarfs erarbeitet wurden.

Ich wünsche Ihnen viel Erfolg bei der Anwendung des IT-Grundschutzes.



Dr. Gerhard Schabhüser

Vize-Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Dankesworte

Die Inhalte des IT-Grundschutz-Kompodiums sind aufgrund der rasanten Entwicklungen in der Informationstechnik sowie immer kürzer werdenden Produktzyklen ständigen Veränderungen ausgesetzt. Neben dem BSI leisten viele Personen einen wertvollen Beitrag, indem sie Texte bis hin zu ganzen Bausteinen für den IT-Grundschutz erstellen, Bausteine kommentieren oder neue Themen anregen.

Folgende Institutionen und Personen haben bei der Bausteinerstellung und -überarbeitung ihr Fachwissen in das IT-Grundschutz-Kompodium einfließen lassen.

IT-Grundschutz-Anwender und -Anwenderinnen

Für die Mitarbeit an der Edition 2023 des IT-Grundschutz-Kompodiums sei an dieser Stelle den zahlreichen IT-Grundschutz-Anwendern und -Anwenderinnen gedankt. Sie haben einzelne IT-Grundschutz-Bausteine kommentiert und ihr Fachwissen in die neue Edition eingebracht.

Mitarbeitende des Bundesamts für Sicherheit in der Informationstechnik

In die aktuelle Überarbeitung des IT-Grundschutz-Kompodiums ist zudem das Fachwissen von zahlreichen BSI-Mitarbeitern und Mitarbeiterinnen eingeflossen. Ihnen gebührt an dieser Stelle besonderer Dank:

Stefan Ahlers, Daniel Balzien, Markus de Brün, Thorsten Dietrich, Dr. Melanie Göbel, Klaus Hunsänger, Vera Lange, Marc Meyer, Andreas Neth, Dr. Frank Niedermeyer, Dr. Harald Niggemann, Detlef Nuß, Dirk Steffes-Enn, Frank Weber, Dr. Dietmar Wippig.

Fortschreibung und Weiterentwicklung vorhergehender Editionen

Auch bei der Fortschreibung und Weiterentwicklung vorhergehender Editionen des IT-Grundschutz-Kompodiums haben zahlreiche Institutionen sowie Personen aus der öffentlichen Verwaltung, Wirtschaft, Wissenschaft und dem BSI mitgewirkt. Auch ihnen sei hiermit Dank ausgesprochen.

Gesamtinhaltsverzeichnis

Vorwort

Dankesworte

Inhaltsverzeichnis

Neues im IT-Grundschutz-Kompendium

IT-Grundschutz – Basis für Informationssicherheit

Schichtenmodell und Modellierung

Rollen

Glossar

Elementare Gefährdungen

- G 0.1 Feuer
- G 0.2 Ungünstige klimatische Bedingungen
- G 0.3 Wasser
- G 0.4 Verschmutzung, Staub, Korrosion
- G 0.5 Naturkatastrophen
- G 0.6 Katastrophen im Umfeld
- G 0.7 Großereignisse im Umfeld
- G 0.8 Ausfall oder Störung der Stromversorgung
- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- G 0.10 Ausfall oder Störung von Versorgungsnetzen
- G 0.11 Ausfall oder Störung von Dienstleistungsunternehmen
- G 0.12 Elektromagnetische Störstrahlung
- G 0.13 Abfangen kompromittierender Strahlung
- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
- G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.24 Zerstörung von Geräten oder Datenträgern
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.33 Personalausfall
- G 0.34 Anschlag
- G 0.35 Nötigung, Erpressung oder Korruption
- G 0.36 Identitätsdiebstahl
- G 0.37 Abstreiten von Handlungen
- G 0.38 Missbrauch personenbezogener Daten

- G 0.39 Schadprogramme
- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.41 Sabotage
- G 0.42 Social Engineering
- G 0.43 Einspielen von Nachrichten
- G 0.44 Unbefugtes Eindringen in Räumlichkeiten
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen
- G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

Prozess-Bausteine

ISMS: Sicherheitsmanagement

- ISMS.1 Sicherheitsmanagement

ORP: Organisation und Personal

- ORP.1 Organisation
- ORP.2 Personal
- ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
- ORP.4 Identitäts- und Berechtigungsmanagement
- ORP.5 Compliance Management (Anforderungsmanagement)

CON: Konzepte und Vorgehensweisen

- CON.1 Kryptokonzept
- CON.2 Datenschutz
- CON.3 Datensicherungskonzept
- CON.6 Löschen und Vernichten
- CON.7 Informationssicherheit auf Auslandsreisen
- CON.8 Software-Entwicklung
- CON.9 Informationsaustausch
- CON.10 Entwicklung von Webanwendungen
- CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

OPS: Betrieb

OPS.1 Eigener Betrieb

OPS.1.1 Kern-IT-Betrieb

- OPS.1.1.1 Allgemeiner IT-Betrieb
- OPS.1.1.2 Ordnungsgemäße IT-Administration
- OPS.1.1.3 Patch- und Änderungsmanagement
- OPS.1.1.4 Schutz vor Schadprogrammen
- OPS.1.1.5 Protokollierung
- OPS.1.1.6 Software-Tests und -Freigaben
- OPS.1.1.7 Systemmanagement

OPS.1.2 Weiterführende Aufgaben

- OPS.1.2.2 Archivierung
- OPS.1.2.4 Telearbeit
- OPS.1.2.5 Fernwartung
- OPS.1.2.6 NTP-Zeitsynchronisation

OPS.2 Betrieb von Dritten

- OPS.2.2 Cloud-Nutzung
- OPS.2.3 Nutzung von Outsourcing

OPS.3 Betrieb für Dritte

- OPS.3.2 Anbieten von Outsourcing

DER: Detektion und Reaktion

- DER.1 Detektion von sicherheitsrelevanten Ereignissen
 - DER.2 Security Incident Management
 - DER.2.1 Behandlung von Sicherheitsvorfällen
 - DER.2.2 Vorsorge für die IT-Forensik
 - DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
 - DER.3 Sicherheitsprüfungen
 - DER.3.1 Audits und Revisionen
 - DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision
- DER.4 Notfallmanagement

System-Bausteine**APP: Anwendungen**

APP.1 Client-Anwendungen

- APP.1.1 Office-Produkte
- APP.1.2 Webbrowser
- APP.1.4 Mobile Anwendungen (Apps)

APP.2 Verzeichnisdienst

- APP.2.1 Allgemeiner Verzeichnisdienst
- APP.2.2 Active Directory Domain Services
- APP.2.3 OpenLDAP

APP.3 Netzbasierte Dienste

- APP.3.1 Webanwendungen und Webservices
- APP.3.2 Webserver
- APP.3.3 Fileserver
- APP.3.4 Samba
- APP.3.6 DNS-Server

APP.4 Business-Anwendungen

- APP.4.2 SAP-ERP-System
- APP.4.3 Relationale Datenbanken
- APP.4.4 Kubernetes
- APP.4.6 SAP ABAP-Programmierung

APP.5 E-Mail/Groupware/Kommunikation

- APP.5.2 Microsoft Exchange und Outlook
- APP.5.3 Allgemeiner E-Mail-Client und -Server
- APP.5.4 Unified Communications und Collaboration (UCC)

- APP.6 Allgemeine Software
- APP.7 Entwicklung von Individualsoftware

SYS: IT-Systeme

SYS.1 Server

- SYS.1.1 Allgemeiner Server
- SYS.1.2 Windows Server
 - SYS.1.2.2 Windows Server 2012
 - SYS.1.2.3 Windows Server
- SYS.1.3 Server unter Linux und Unix
- SYS.1.5 Virtualisierung
- SYS.1.6 Containerisierung
- SYS.1.7 IBM Z
- SYS.1.8 Speicherlösungen
- SYS.1.9 Terminalserver

SYS.2 Desktop-Systeme

- SYS.2.1 Allgemeiner Client
- SYS.2.2 Windows-Clients
 - SYS.2.2.3 Clients unter Windows
- SYS.2.3 Clients unter Linux und Unix
- SYS.2.4 Clients unter macOS
- SYS.2.5 Client-Virtualisierung
- SYS.2.6 Virtual Desktop Infrastructure

SYS.3 Mobile Devices

- SYS.3.1 Laptops
- SYS.3.2 Tablet und Smartphone
 - SYS.3.2.1 Allgemeine Smartphones und Tablets
 - SYS.3.2.2 Mobile Device Management (MDM)
 - SYS.3.2.3 iOS (for Enterprise)
 - SYS.3.2.4 Android
- SYS.3.3 Mobiltelefon

SYS.4 Sonstige Systeme

- SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
- SYS.4.3 Eingebettete Systeme
- SYS.4.4 Allgemeines IoT-Gerät
- SYS.4.5 Wechseldatenträger

IND: Industrielle IT

- IND.1 Prozessleit- und Automatisierungstechnik
- #### IND.2 ICS-Komponenten
- IND.2.1 Allgemeine ICS-Komponente
 - IND.2.2 Speicherprogrammierbare Steuerung (SPS)
 - IND.2.3 Sensoren und Aktoren
 - IND.2.4 Maschine
 - IND.2.7 Safety Instrumented Systems
- #### IND.3 Produktionsnetze
- IND.3.2 Fernwartung im industriellen Umfeld

NET: Netze und Kommunikation

NET.1 Netze

- NET.1.1 Netzarchitektur und -design
- NET.1.2 Netzmanagement

NET.2 Funknetze

- NET.2.1 WLAN-Betrieb
- NET.2.2 WLAN-Nutzung

NET.3 Netzkomponenten

- NET.3.1 Router und Switches
- NET.3.2 Firewall
- NET.3.3 VPN
- NET.3.4 Network Access Control

NET.4: Telekommunikation

- NET.4.1 TK-Anlagen
- NET.4.2 VoIP
- NET.4.3 Faxgeräte und Faxserver

INF: Infrastruktur

- INF.1 Allgemeines Gebäude
- INF.2 Rechenzentrum sowie Serverraum
- INF.5 Raum sowie Schrank für technische Infrastruktur
- INF.6 Datenträgerarchiv
- INF.7 Büroarbeitsplatz
- INF.8 Häuslicher Arbeitsplatz
- INF.9 Mobiler Arbeitsplatz
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume
- INF.11 Allgemeines Fahrzeug
- INF.12 Verkabelung
- INF.13 Technisches Gebäudemanagement
- INF.14 Gebäudeautomation

Neues im IT-Grundschutz-Kompodium

Die Edition 2023 des IT-Grundschutz-Kompodiums enthält insgesamt 111 IT-Grundschutz-Bausteine. Darunter sind zehn neue IT-Grundschutz-Bausteine sowie 101 Bausteine aus der Edition 2022. Drei Bausteine aus der Edition 2022 sind entfallen. Aus der Edition 2022 wurden 21 Bausteine für die Edition 2023 überarbeitet.

Neue Bausteine

Die folgenden 10 neuen IT-Grundschutz-Bausteine sind in fünf unterschiedlichen Schichten hinzugekommen:

- CON.11.1 *Geheimchutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)*
- OPS.1.1.1 *Allgemeiner IT-Betrieb*
- OPS.2.3 *Nutzung von Outsourcing* (dieser Baustein ersetzt OPS.2.1 *Outsourcing für Kunden*)
- OPS.3.2 *Anbieten von Outsourcing* (dieser Baustein ersetzt OPS.3.1 *Outsourcing für Dienstleister*)
- APP.5.4 *Unified Communications und Collaboration (UCC)*
- SYS.1.2.3 *Windows Server*
- SYS.1.9 *Terminalserver*
- SYS.2.5 *Client-Virtualisierung*
- SYS.2.6 *Virtual Desktop Infrastructure*
- NET.3.4 *Network Access Control*

Entfallene Bausteine

Die folgenden Bausteine sind in der Edition 2023 entfallen:

- SYS.2.2.2 *Clients unter Windows 8.1*: Der Support für das Betriebssystem endete am 10.01.2023. Windows 8.1 sollte daher nicht mehr eingesetzt werden.
- OPS.2.1 *Outsourcing für Kunden*: Der Baustein wird durch OPS.2.3 *Nutzung von Outsourcing* ersetzt
- OPS.3.1 *Outsourcing für Dienstleister*: Der Baustein wird durch OPS.3.2 *Anbieten von Outsourcing* ersetzt

Überarbeitete Bausteine

Nach der Veröffentlichung der letzten Edition des IT-Grundschutz-Kompodiums im Februar 2022 hat das IT-Grundschutz-Team zahlreiche wertvolle Rückmeldungen von IT-Grundschutz-Anwendern und -Anwenderinnen erhalten. Hinweise zu einzelnen Aspekten und Erfahrungswerte aus der beruflichen Praxis von Informationssicherheitsbeauftragten sowie weiteren erfahrenen Anwendenden tragen dazu bei, die Inhalte noch aktueller und praxistauglicher aufzubereiten. Die einzelnen Bausteintexte wurden daraufhin gesichtet und überarbeitet, sodass in der Edition 2023 21 IT-Grundschutz-Bausteine aktualisiert wurden.

Die IT-Grundschutz-Bausteine sind in einem unterschiedlichen Umfang überarbeitet worden. Die Änderungen sind wie folgt klassifiziert:

- **Umfangreiche Änderungen**, die Auswirkungen auf Zertifizierungsverfahren oder bestehende Sicherheitskonzepte haben können, sind in separaten Änderungsdokumenten aufgeführt. Dies betrifft 21 Bausteine aus der Edition 2022. Die „Änderungsdokumente (Edition 2023)“ sind auf der BSI-Webseite in der Rubrik IT-Grundschutz-Kompodium veröffentlicht.
- **Geringfügige sprachliche und redaktionelle Änderungen** sowie Überarbeitungen aus Gründen der besseren Verständlichkeit werden nicht in einem separaten Änderungsdokument aufgeführt. Bei IT-Grundschutz-Bausteinen, die entsprechend geringfügig bearbeitet wurden, ist lediglich das Datum in der Fußzeile auf die aktuelle Edition gesetzt worden. Dies betrifft alle Bausteine aus der Edition 2022, die nicht umfangreich geändert wurden.

IT-Grundschutz-Bausteine aus der Edition 2022, die überarbeitet wurden und zu denen ein Änderungsdocument verfügbar ist:

- ORP.1 *Organisation*
- CON.1 *Kryptokonzept*
- CON.2 *Datenschutz*
- OPS.1.1.2 *Ordnungsgemäße IT-Administration*
- OPS.1.1.3 *Patch- und Änderungsmanagement*
- OPS.1.2.5 *Fernwartung*
- APP.1.2 *Webbrowser*
- APP.2.1 *Allgemeiner Verzeichnisdienst*
- APP.2.2 *Active Directory*: Der Baustein wurde in „*Active Directory Domain Services*“ umbenannt
- APP.2.3 *OpenLDAP*
- APP.5.3 *Allgemeiner E-Mail-Client und -Server*
- SYS.1.1 *Allgemeiner Server*
- SYS.2.1 *Allgemeiner Client*
- SYS.2.3 *Clients unter Linux und Unix*
- SYS.2.2.3 *Clients unter Windows 10*: Der Baustein wurde in „*Clients unter Windows*“ umbenannt und behandelt nun mit Windows 10 und 11 die einzigen beiden Versionen von Windows für Client-Systeme, die durch Microsoft Support erhalten.
- SYS.4.3 *Eingebettete Systeme*
- SYS.4.5 *Wechseldatenträger*
- IND.3.2 *Fernwartung im industriellen Umfeld*
- INF.1 *Allgemeines Gebäude*
- INF.2 *Rechenzentrum sowie Serverraum*
- INF.10 *Besprechungs-, Veranstaltungs- und Schulungsraum*

Überarbeitung von Rollen

Folgende Rollen wurden mit der Edition 2023 umbenannt:

Alte Rollenbezeichnung	Neue Rollenbezeichnung
Anforderungsmanager (Compliance Manager)	Compliance-Beauftragte
Bauleiter	Bauleitung
Benutzer	Benutzende
Bereichssicherheitsbeauftragter	Bereichssicherheitsbeauftragte
Brandschutzbeauftragter	Brandschutzbeauftragte
Datenschutzbeauftragter	Datenschutzbeauftragte
Entwickler	Entwickelnde
ICS-Informationssicherheitsbeauftragter	ICS-Informationssicherheitsbeauftragte
Informationssicherheitsbeauftragter (ISB)	Informationssicherheitsbeauftragte (ISB)
Mitarbeiter	Mitarbeitende
Notfallbeauftragter	Notfallbeauftragte
OT-Leiter	OT-Leitung
Planer	Planende
Tester	Testende

Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

Aktualisierungen aller Kreuzreferenztabellen und strukturelle Anpassung der Bausteine

Alle Bausteine der Edition 2022 wurden für die Edition 2023 strukturell überarbeitet.

Die Kreuzreferenztabellen, die die Anforderungen jedes Bausteins den elementaren Gefährdungen gegenüberstellen, wurden geprüft und überarbeitet. Zukünftig zeigen diese nur noch direkte Gefährdungen, die unmittelbar auf das Zielobjekt einwirken und die durch die Anforderungen aus dem Baustein behandelt werden. Hierbei werden nur noch direkte Beziehungen zwischen Elementaren Gefährdungen und Anforderungen aufgeführt. Indirekte Beziehungen, die aus direkten Beziehungen folgen, wurden entfernt. Dadurch steigt die Übersicht und der eindeutige Fokus wird auf die für das Zielobjekt relevanten Gefährdungen gesetzt. Durch die Überarbeitung entsteht weniger Aufwand, wenn die Kreuzreferenztabellen für eine Risikoanalyse genutzt werden.

Die Elementaren Gefährdungen, die für den jeweiligen Baustein relevant sind, werden nun nur noch in den Kreuzreferenztabellen aufgeführt. Diese werden separat auf den Webseiten des BSI veröffentlicht. Die Anlage „Kreuzreferenztafel zu elementaren Gefährdungen“ wurde in den einzelnen Bausteinen entfernt.

Errata und überarbeitete Bausteine

Trotz einer sorgfältigen, mehrstufigen Qualitätssicherung lassen sich Fehler und Unschärfen bei einem Werk vom Umfang des IT-Grundschutz-Kompodiums nicht immer vermeiden. Auch können aufgrund der schnellen Entwicklungszyklen in der Informationstechnik Konzepte und Anforderungen aus dem IT-Grundschutz zum Erscheinungsdatum der jeweiligen Edition nicht mehr vollständig zutreffen.

Anwendende, denen Fehler oder Probleme auffallen, sind dazu eingeladen, diese an it-grundschutz@bsi.bund.de zu melden. Alle Anmerkungen werden durch das IT-Grundschutz-Team geprüft und fließen geeignet in die nächste Edition des IT-Grundschutz-Kompodiums ein.

Im Jahresverlauf können außerdem Drafts von überarbeiteten Bausteinen erscheinen, die bereits entsprechend aktualisiert sind.

Notwendige Korrekturen, die nach Redaktionsschluss der aktuellen Edition auftreten, werden (falls vorhanden) in den „Errata zur Edition 2023“ auf den IT-Grundschutz-Webseiten unter <https://bsi.bund.de/grundschutz> in der Rubrik „IT-Grundschutz-Kompodium“ veröffentlicht. Sie ersetzen anderslautende Aussagen im IT-Grundschutz-Kompodium.

Geschlechtergerechtere Sprache

Im Sinne der Gleichbehandlung wurden für die Edition 2023 alle Bausteine des IT-Grundschutz-Kompodiums in eine geschlechtergerechtere Sprache überführt.

